Chapter 13. Decentralized Finance: the Future of Crypto and Open Finance ?[1] [2]
Forthcoming in Linda Jeng's Introduction to Open Banking, OUP
Nic Carter[3]

1. Introduction

In parallel to the open banking and growing open finance phenomena described in this book, a related but distinct movement is taking place - the rise of decentralized finance built atop crypto-financial infrastructure. By this, we refer to the provision of a subset of financial services through smart contracts[4] and tokens circulating on public blockchains. Unlike open banking which seeks to link disparate bank ledgers, through bridging technology either by market forces or government mandate, decentralized finance aims to unite a global, jurisdiction-independent userbase on shared, public ledgers. Attempting to substitute standard legal protections with *lex cryptographia,*[5] decentralized finance entrepreneurs envision an open source set of financial experiences in which end-users can audit and verify the very software code they are entrusting their assets to.

While decentralized finance or "DeFi" is distinct from open finance, it shares many of its key traits and surpasses them in certain respects:

- developers can build and deploy value-bearing contracts to public blockchains without permission and without a traditional contractual relationship with end-users;
- end-users can freely move from one smart contract-based product to another, as keypairs are substituted for identity; and,
- the interlinking smart contracts that mediate these experiences are open source and auditable. Chiefly these products are on platforms that aim to be permissionless (to both develop on and get access to), interoperable, auditable, and trust-minimized,[6] satisfying these qualities to various degrees.

Fundamentally, the DeFi sector aspires to flatten the topology of finance and return margins that might be captured by financial institutions to end-users as a consumer surplus. The sector

---

[1] Disclaimer: The author's firm has an active position in Bitcoin. All mentions of protocols, tokens, and digital assets in this chapter are merely exemplary and do not constitute endorsements

[2] The author would like to thank Alex Treece and David Hoffman for their feedback and contributions to this article

[3] Partner at Castle Island Ventures

[4] 'Smart contracts' refers to programmatically codified relationships over property, with automated enforcement of terms. They can cover a subset of cases that are highly codifiable - for instance, a financial derivative. for more nebulous contracts like for instance a SAFE note, they obviously wouldn't substitute. See Nick Szabo. "Smart Contracts: Building Blocks for Digital Markets." Unpublished manuscript (1996). Available at https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html

[5] It is still to be seen how legal courts would view blockchain transactions serving as a form of law. For more on how public blockchains can be understood as an alternative legal regime, see Wright, Aaron, and Primavera De Filippi, "Decentralized blockchain technology and the rise of lex cryptographia." Available at SSRN 2580664 (2015)

[6] "Trust minimization" refers to reducing the amount of trust that a user must place in specific entities to feel secure using a financial system, product or service.

is premised on an ideology of disintermediation, with apolitical protocols and clearly stipulated rules (defined in code) deemed preferable to traditional financial intermediaries. Its popularity can be understood as a reaction to restrictions on various classes of financial activity, imposed either by risk-averse bank sectors, or to government-imposed restrictions on capital formation and flows.

The DeFi sector is still incipient but is growing rapidly and has caught the attention of policymakers. Its highly open and permissionless approach is both the core value proposition and a potential catalyst for regulatory attention. But the scope and nature of financial activity taking place in this permissionless, open source context should command attention. DeFi promotes a far less constrained, far more interoperable, and directly auditable version of financial services from which open banking enthusiasts can take lessons. Already, the DeFi sector has begun converging with the traditional, regulated financial sector, presaging a possible world in which public blockchains are seamlessly incorporated into established financial networks as alternative payments and settlement rails. This transition might however compromise the features of decentralized finance that its adherents find so valuable – a lack of transactional encumbrances, the absence of identity from the system, and the permissionless deployment of certain financial contracts.

As an industry premised on digital bearer[7] assets, DeFi introduces novel classes of risk, many of which are still poorly understood. Additionally, the specter of both reintermediation and the desire for points of centralization by financial regulators grappling with the sector threatens to derail DeFi industry objectives. This chapter also explores some of these systemic risks and trends that will impact open finance.

2. Defining 'DeFi'

While the term 'DeFi' can be used to generally refer to all permissionless financial applications relying on public blockchains - the cryptocurrency industry views, 'DeFi' as a term of art that refers more specifically to derivative contracts deployed on smart contract blockchains that facilitate asset swaps, programmatic leverage, and risk transformation. Arguably, however, to the extent that facilitating the conveyance of value on public platforms - that exist on thousands of nodes globally and rely on a distributed base of industrial validators - can be understood as finance, even the most basic features of a blockchain like Bitcoin,[8] which is largely single-purpose, can fall under the decentralized finance moniker. Under this broader definition, 'decentralized finance' captures all financial activity occurring on public blockchains; the narrower definition would limit the scope, perhaps too narrowly, to trust-minimized 'high finance' facilitated by contracts on-chain, including the on-chain creation of derivatives, asset swaps, leverage, insurance, and other forms of risk transformation. I focus on the narrower

[7] I view these digital assets as bearer-like even though - unlike with cash - ownership can be recorded on blockchain. I call them 'digital bearer assets' because, instead of ownership through title registration, knowledge of the digital assets' keys is tantamount to ownership of the digital assets.

[8] We capitalize the term 'Bitcoin' the network and protocol, and lowercase 'bitcoin' when referring to the asset.

definition in this chapter, but expect the definition will be better reflected by the broader version, which will also inevitably converge with aspects of open finance.

a. Decentralized exchanges (DEXs) of “pseudo-equity"

Due to the growth of third-party financial assets – (initially ‘utility tokens’[9] but increasingly “pseudo-equity”[10]) – alongside fiat-pegged tokens (which are more suitable as a medium of exchange), smart contract-optimized blockchains like Ethereum have been able to cultivate a rich environment of exchanges “on-chain.” These on-chain exchanges refer to exchange products that enable users to find counterparties and settle without depositing assets with a third-party exchange. Instead, users engage in trades through smart contracts, which settle directly on the blockchain without ever surrendering custody.

While these products are referred to as “decentralized exchanges” or DEXs, it is simpler to understand these not as exchange venues but rather as a form of bilateral or multilateral trade, facilitated by software, between mutually- consenting parties. As Coin Center’s Peter Van Valkenburgh describes it:,[11]

> *Calling those tools “a DEX” and referring to “DEXs” as a category of things that exist in the world (rather than actions) does the entire technology a disservice: it wrongly portrays software tools as persons or businesses with agency and legal obligations. Corporations and persons — legal or natural — definitely have agency and obligations; software tools do not. Corporations and persons can be held responsible for their actions, software tools cannot.*

Under this interpretation, users do not use a DEX product the same way they use a centralized securities exchange; instead, they use public software tools to find acceptable terms for an asset swap with contracts deployed on the blockchain itself to handle execution and settlement. The DEX phenomenon is further explained below in section 4(c).

3. Overview: comparing Blockchain-based DeFi with Open Finance

Before describing DeFi in more detail, I want to provide an overview of how the DeFi movement and open finance are motivated by similar goals of improving the competitive landscape, including a desire to improve financial inclusion by reducing switching costs and making user data (or assets, in the case of DeFi) more portable. They accomplish this in disparate ways.

---

[9] ‘Utility tokens’ are effectively digital arcade tokens that are presumed to accrue value due to their required usage in a product or marketplace; the theory being that sufficient utility will manifest in stable financial value.

[10] By ‘pseudo-equity’, we refer to tokens that entitle token holders to control rights over economically-valuable property (typically a smart contract), and in some cases, cash flows deriving from that property. These tokens are not issued as registered securities offerings, but are rather issued directly to a global audience of investors through public blockchain infrastructure.

[11] See Peter Van Valkenburgh, “There’s no such thing as a decentralized exchange,” The Block (Oct. 3 2020). Available at https://www.theblockcrypto.com/amp/post/79768/theres-no-such-thing-as-a-decentralized-exchange

Open finance involves either mandating financial institutions to unencumber user-permissioned data in order to enhance competition; or alternatively, building interoperation between incumbent firms and fintech entrants that is enhanced by private sector solutions. DeFi, by contrast, does not seek to link multiple financial databases through either private sector agreement or state mandate, but instead envisions an entirely novel financial system where a global userbase is united on one database – the ledger maintained by the blockchain. Additionally, the core service providers are not financial institutions, but rather contracts deployed to these blockchains. In theory, since duplicating and iterating on open-source code is trivial, and switching from one liquidity pool to the next is seamless,[12] users are empowered to decide where to conduct activities and rents are difficult to collect.

a. Crypto interoperability

In practice, the crypto-financial industry remains somewhat fragmented as there are multiple popular blockchains that do not cleanly interoperate. Partial solutions like "wrapping" Bitcoin, mainly through intermediaries, and tokenizing it on Ethereum have sprung up, but these interoperability solutions are, for the most part, not trust-minimized.[13] Additionally, it is not clear whether, under current trust assumptions, a single blockchain can scale to a global userbase of retail transactors.[14] As the default choice for DeFi applications, Ethereum is at capacity and experienced a surge of fees in 2020 that priced out smaller users, rendering only larger transactions in value viable.

b. Clear settlement v. scaling

Numerous proposals exist to increase the throughput of these systems, but a fundamental tension remains in trying to scale DeFi. Scaling blockchains by deferring settlement would preclude the convenient DeFi features associated with settling on the blockchain. Alternatively, scaling by producing numerous distinct ledgers would lead to fragmentation, inhibiting the core idea that powers DeFi – the notion of uniting transactors on a single ledger. This tension gets to the heart of an embedded paradox troubling the DeFi phenomenon: the touted benefits of uniting transactors on a single ledger would become meaningless if scaling public blockchains meant only a network of distinct ledgers that have to periodically communicate and settle with

[12] One infamous example would be the hostile fork (or clone) of Uniswap, the popular DEX by its competitor Sushiswap. Within a week of launching, Sushiswap had attracted $1.4b worth of liquidity, much of it siphoned from Uniswap (Sushiswap offered temporarily better terms to liquidity providers). This provoked outcry, but fundamentally these smart contracts are simply code deployed on blockchains, and can be trivially replicated and modified. This means that successful products are aggressively forked and iterated upon by competitors without restriction.

[13] See fn. 5 for definition of "trust-minimization".

[14] Since the standard trust assumptions of public blockchains require that an individual be able to replay the entire history of transactions and stay current with new transactions as they are added to the chain tip, merely increasing the data throughput of the system in order to scale to a global userbase is infeasible; it would rapidly eliminate the ability of transactors to verify the validity of inbound transactions. Thus, scaling approaches generally involve creating subledgers, deferring settlement, or bundling transactions off-chain and periodically settling on-chain.

each other. Already interoperability challenges are emerging, as Ethereum groans under the weight of its own transactional usage and users look to alternative smart contract protocols.

c. Open access

Despite these tensions, it is worth pointing out the domains in which DeFi shines when evaluated from an open finance lens. First, due to the general lack of identity within public blockchain systems, DeFi solutions are not opinionated in terms of who can access and use them. This open access can be understood as generally positive for financial inclusion (for individuals in countries with poor access to the financial system and seeking to earn USD-denominated yield, for instance). But open access is also a key risk factor as it opens up the DeFi system to illicit usage. Importantly, inasmuch as DeFi solutions are simply smart contracts that users can freely interact with, accounts are inherently portable. Withdrawing funds from an interest-bearing pool and moving them to another pool is seamless. The commitment to neutral financial *protocols* rather than financial service providers promises to inculcate a competitive dynamic whereby entrepreneurs compete to provide popular interfaces based on shared underlying blockchain infrastructure.

d. Composability

Additionally, the combination of strong settlement finality[15] and the concentration of activity onto a single ledger enables the highly desirable quality of composability. As stated, a highly composabe system is one in which distinct components can build upon and reference each other, allowing for complexity and more sophisticated products to emerge. With composability, certain DeFi applications might refer to or rely on a half dozen other systems within a relatively short period. While this has the potential to introduce systemic risk, and cascading failures if individual components or modules fail, it also allows for the creation of abstractions and novel financial products.

We will sketch out an example[16] to demonstrate the level of composability currently exhibited on DeFi. The yEarn protocol is an on-chain asset manager, which pools users' funds and deploys them against a variety of strategies in order to obtain a return. The yETH vault is one of the

[15] Final transactions are those which are not reversible. Physical cash transactions, for instance, settle immediately, whereas credit card transactions are not final for the period in which they can be contested. Public blockchains offer 'probabilistic' finality, which means that transactions are presumed to be final once the ledger has accumulated sufficient computational work, such that a reversal would be implausible or expensive. For additional explanation on finality, see Elaine Ou, "Cryptocurrency Deals Can Always Be Erased, for a Price", *Bloomberg*. (Jan. 16, 2019). https://www.bloomberg.com/opinion/articles/2019-01-16/bitcoin-and-other-cryptocurrencies-are-open-about-being-at-risk

[16] The inclusion of this example does not reflect the author's views on the viability of these products. For more details on the processes described in this section, see Andre Cronje, "yETH vault explained," available at https://medium.com/iearn/yeth-vault-explained-c29d6b93a371 (Sep. 4 2020); and Yearn.Finance, "yETH Vault Mechanics," available at https://docs.yearn.finance/products/yvaults#yeth-vault-mechanics. At its peak, yearn.finance managed $967m in user deposits in strategies like these (see: https://defipulse.com/yearn.finance)

products offered by yEarn in which users deposit Ether (ETH) and the system endeavors to seek a return with those funds. yEarn works by taking Ether deposits from users, bundling them together, and depositing them into the Maker contract, using this Ether collateral to produce Dai, a dollar-denominated stablecoin. At this point, the Dai (effectively a loan granted by the Maker system against risky Ether collateral) is then deposited into the Curve.fi liquidity pool as a source of liquidity, and yEarn thus becomes a liquidity provider. Curve is a decentralized exchange optimized for stablecoins. Liquidity providers putatively earn a return for making markets – and are also rewarded with the local pseudo-equity token in the Curve system, CRV, which is subsequently sold for ETH by yEarn.

To summarize, this process entails an asset manager transparently pooling user funds, depositing these pooled funds into an overcollateralized[17] lending system to create a dollar-denominated token (Dai), which is then subsequently deposited into a decentralized exchange to provide liquidity for automated market making, a compensated activity (assuming the market-making is profitable). These tokens then (optimistically) earn a return, and the individuals depositing into the initial pool collect a yield. This process combines a number of entirely distinct modules, each expressed as code deployed on the network Ethereum. Developers of one module do not need to be aware of third parties using their protocol. Permission is neither sought nor required.

e. Auditability

Another touted advantage of DeFi from an open finance perspective is its auditability. Due to the innate transparency of public blockchains, data from these systems can be queried by any third-party running a node. This allows for risks, especially with regards to collateral quality, to be evaluated in real time. Using publicly-accessible blockchain data, service providers are now developing automated risk scoring protocols[18] to assess collateral quality and system solvency in various lending products. Of course, this also means that end-users have a lack of privacy when transacting on DeFi, indelibly so if their identity can be connected to their blockchain address.

f. "Bearer-like"

DeFi protocols are generally built with user self-custody in mind, and cryptoassets are intended to be "bearer-like" and fungible. Analogous to the physical possession of cash, the mere knowledge of the cryptoasset's private key entitles the individual the ability to spend the cryptoassets, thus making the individual the genuine owner of the cryptoassets in the eyes of the blockchain protocol. However, cryptoassets differ in significant ways from typical bearer

[17] The minimum collateral ratio is 150%.

[18] See for example Gauntlet's real-time risk management product, discussed by John Morrow, "Risk Scores for DeFi— Alpha Release" (Oct. 13, 2020), available at https://medium.com/gauntlet-networks/understanding-risk-in-defi-f64574593979

instruments, such as cash,[19] which maintains no ownership record and for which physical possession entitles the bearer ownership or title. Unlike cash, cryptoassets are linked to a form of identity and can therefore maintain a record of ownership.

These blockchain protocols generally presume that the assets are fungible and "bearer-like". However, these core assumptions break down once identity link via private keys is introduced and individuals or parties are associated with their addresses. For example, liquidity pools in MKR or Compound require collateral fungibility. In other words, they cannot tolerate different classes of risk based on who is providing liquidity. Many defi enthusiasts hope that eventually privacy tools will enable genuine fungibility for the collateral flowing around the DeFi system.)

g. Portability

Lastly, while depository relationships with banks or brokers tend to be long-term and 'sticky', , users in the blockchain context can take physical receipt of their cryptoassets and move them with little difficulty. This ease of portability is generally challenging or not possible with other types of asset classes, particularly securities. Blockchain's portability feature has the emergent consequence of enabling collateral to flow rapidly between DeFi protocols. A typical end-user might retain ownership of their keys and interact with contracts registered to the blockchain through a software or hardware interface that enables the user to sign transactions safely – instead of consigning the user's assets to a third-party and granting control to an agent.

4. Public blockchains and decentralized finance

After the above introductory comparative overview, this section explores certain key aspects of DeFi in more detail but does not dwell on the technical features of the public blockchains that power DeFi. (For introductory works covering how blockchains function, see Narayanan, Antonopoulos, or Rosenbaum.[20]) Nevertheless, there are some important features of blockchains worth revisiting in this context, to help us identify the differences between modes of user engagement with public blockchains and with traditional banking systems and, ultimately, with open finance.

a. Bitcoin

A blockchain using Proof-of-Work, such as Bitcoin, is a protocol that cultivates a shared, continually-updated global ledger upon which participants converge. This type of blockchain stipulates which addresses can spend which coins and under which conditions as well as

---

[19] For example, cash, bearer's bonds, negotiable instruments made payable to "bearer", etc.

[20] See Narayanan, Arvind, et al. *Bitcoin and cryptocurrency technologies: a comprehensive introduction*. Princeton University Press, 2016; Antonopoulos, Andreas M. *Mastering Bitcoin: unlocking digital cryptocurrencies.* " O'Reilly Media, Inc.", 2014; and Antonopoulos, Andreas M., and Gavin Wood. *Mastering ethereum: building smart contracts and dapps*. O'reilly Media, 2018.

facilitate transactional finality when updates occur. Identity is deliberately absent from the system, with pseudonymous public-key addresses serving as a substitute. Users do not need to register with a third party to use Bitcoin; they must simply generate sufficient randomness to construct a unique secret in order to devise a pair of public and private keys. If the randomness is sufficiently unique, the user can plausibly assert that they alone are the sole proprietor of that data and hence the coins, which are encumbered and linked to their address. Knowledge of the private key with a corresponding public key, which contains value in an output on the Bitcoin ledger, entitles you to spend those coins.

Private keys do not "store" units of bitcoin; the units of bitcoin can be said to exist on the virtualized ledger replicated across thousands of nodes globally, which reach periodic synchrony[21]. Keys are merely an entitlement to unlock coins and assign them to a new address. In this manner, bitcoin is "bearer-like" as discussed earlier. Units of bitcoin are not redeemable (as, for instance, a banknote used to be redeemable for gold), but knowledge of a private key is the sole determinant of a valid spend on the blockchain even if that knowledge was obtained illicitly. There is no recourse on Bitcoin, and transactions are final after sufficient block confirmations. In this respect, Bitcoin resembles cash in an online context; it is somewhat (albeit not perfectly) private, settlement is rapidly final, and transactors have full autonomy with whom they transact.

In blockchain transactions, it is the receiving party's responsibility to verify the integrity of the transaction. Verifying that an inbound Bitcoin transaction is legitimate entails downloading the history of the ledger from the P2P network[22], double-checking that all bitcoin transactions or "spends" are valid to prevent double-spending, and confirming that all new bitcoins were created fairly under network rules. By operating a node on consumer hardware, a user could cheaply determine that a payment they are receiving is final (according to their self-directed standard of probabilistic settlement finality) and not counterfeit. More importantly, they can conduct this validation for themselves without relying on any trusted third party, and without trusting their transactional counterparty. This grants Bitcoin the quality of being able to settle payments rapidly on a cross-jurisdictional basis between parties that do not trust each other and may not even have knowledge of each other, much less a relationship.

Transactions are broadcast to miners who arrange them in blocks and register them to the final blockchain, in exchange for conducting economically-costly computational work. Mining is a competitive, free market activity in which industrial entities compete for the privilege of bundling and registering transactions to the blockchain. They are compensated with a bitcoin-denominated reward consisting of a protocol-defined subsidy as well as transaction fees, which

---

[21] Bitcoin's trust model requires that nodes agree on a single, unified state of the world, such that transactors cannot spend the same coins with multiple parties at the same time. Thus, nodes in the network collectively update their state every 10 minutes, on average.

[22] It is currently about 304 GB in size as of October 2020. a transaction that you are the recipient of. party A submits a transaction to the blockchain, reassigning coins to party B. it's B's responsibility to verify the integrity of the transaction (by running a full node which trustlessly consults the blockchain).

are set by a first-price auction. They are economically-incentivized to include user transactions that they receive from nodes because these transactions are fee-bearing. Miners have full discretion over the transactions they choose to include in blocks, and individual miners can censor specific addresses should they choose or even mine fully empty blocks; but the free market nature of mining suggests that another miner would eventually select the excluded transaction in exchange for the fee.

That said, a miner with an overwhelming share of hashpower could arbitrarily censor transactions and otherwise interfere with the network. A competitive and distributed mining environment is a core assumption that must hold for the network to function in an orderly manner. So far, no individual miner or entity has obtained sufficient market share to interfere with the network; nor would they be economically-incentivized to because they have exposure to the Bitcoin network through their single-purpose mining hardware, which depreciates over a period of years. Thus, any damage to the bitcoin unit price on account of malicious behavior would punish them economically, since miners hold on their balance sheet synthetic future units of bitcoin instantiated in mining hardware.[23]

For end-users to have the confidence that they will have access to the network and will be able to transact, they must believe that the free market competition for transaction registration is sufficient to enforce a heterogeneity and non-cartelized set of entities. If real-world user identities can be linked with their addresses and transactions, and the validator network becomes cartelized, the network assurances become impaired as miners at this point can censor end-users. This quality of excludability might be a desirable feature of a financial network in the eyes of regulators, but Bitcoin's core value proposition is a censorship-resistant network for conveying and storing value without the aegis of any legal system,[24] and this is fundamentally why it is valued by end-users. Thus, compromising on those features by, for instance, adding KYC (Know-Your-Customer) procedures at the address level, or regulating the transactions that miners are permitted to register to the blockchain, is incompatible with the network's established goals.

Bitcoin is both a monetary and financial phenomenon, by its creator's intention[25] and its revealed trajectory since launch. Bitcoin is a financial technology inasmuch as it facilitates final settlement of value between mutually untrusting counterparties through a communications

---

[23]See Hasu, James Prestwich, and Brandon Curtis. "A Model for Bitcoin's Security and the Declining Block Subsidy." (2019). Available at https://medium.com/@hasufly/research-paper-a-model-for-bitcoins-security-and-the-declining-block-subsidy-11a21f600e33

[24] See Yassine Elmandjra, "Bitcoin: A Novel Economic Institution" Ark Invest (2020), and Eric Chason, "How Bitcoin Functions As Property Law." *Seton Hall L. Rev.* 49 (2018): 129.

[25] In announcing Bitcoin to the cryptography mailing list, Bitcoin creator Satoshi Nakamoto characterized it as a monetary network, emphasizing the fixed supply characteristics (see: Bitcoin v0.1 Released, available at https://satoshi.nakamotoinstitute.org/emails/cryptography/16/). Satoshi also compared Bitcoin to gold, stating that "it's more typical of a precious metal" on the P2P foundation website (see: Bitcoin open source implementation of P2P currency, available at https://satoshi.nakamotoinstitute.org/posts/p2pfoundation/3/#selection-9.0-12.0)

medium. It is monetary in that it is opinionated about monetary policy and boasts clearly-defined monetary rules, which are presumed to be sound and immutable. Non-monetary use cases of Bitcoin have been the source of controversy[26] and are generally deprioritized by developers and protocol design. The Bitcoin protocol is chiefly interested in cultivating its own UTXO[27] set – the set of virtual bills that hold value. After about 12 years of operation, there are 68 million UTXOs summing up to 18.5 million BTC – the units of digital currency represented on the ledger – held in 31.8 million unique nonzero addresses, of which about a million are active on a typical day.

Bitcoin also includes a rudimentary scripting language, which enables the inclusion of more specialized spending conditions in transactions; users can for instance specify that an output must be a certain age to be spent, or require a quorum from a certain number of keys to be spendable, or require that a spender must have knowledge of some specific data to spend the coins.

Bitcoin's native script, called Bitcoin Script, is a variant of the stack-based Forth programming language. It is deliberately limited and not Turing-complete,[28] which means that it cannot perform arbitrary computation. This is done out of prudence, as more expressivity could introduce bugs, and because the Bitcoin protocol is focused on mediating the transfer of units of bitcoin, rather than anything else. Bitcoin's scripting abilities constitute primitives – basic programming building blocks – which allow for the construction of more creative financial instruments like derivatives or transactions, which encode specific conditions. Currently, conditions expressed in these scripts define the spending conditions for a large fraction of outstanding coins.

At present, 5.85 million BTC (equivalent to $66.6 billion USD at the time of writing) are encumbered in "pay to script hash" outputs, meaning that these coins have specific spending conditions attached to them. By inspecting the blockchain, it is possible to know that, for instance, at least 211,000 BTC are publicly revealed to be held in outputs, which require the presence of at least two out of three predetermined signatures to be spent.[29] Such multi-signature transactions are one basic building block of decentralized finance as they permit more complex transactional and trust arrangements to be developed.

However, since Bitcoin Script is challenging to interpret and program with, and not Turing-complete, more expressive protocols like Ethereum were developed. It is Ethereum's

---

[26] See OP_RETURN, Bitcoin Wiki. Available at https://en.bitcoin.it/wiki/OP_RETURN#:~:text=OP_RETURN%20is%20a%20script%20opcode,be%20used%20to%20burn%20bitcoins.

[27] UTXO stands for Unspent Transaction Output. Bitcoin transactions contain bundles of valid UTXOs. Think of these like virtual bills holding variable amounts of value. Bitcoin is a token-based, not an account-based, system. The protocol manages the conveyance of these outputs.

[28] Turing completeness means that a computer or language can be used to conduct arbitrary computation

[29] See "P2SH Statistics" at TxStats. Available at https://txstats.com/dashboard/db/p2sh-statistics

blockchain that hosts most of the popular decentralized finance applications, alongside a handful of other similarly expressive protocols more optimized for smart contracts.

b. Ethereum

In many respects, Ethereum is similar to Bitcoin as described above: identity is largely expunged from the system, and knowledge of a private key is tantamount to ownership. Like Bitcoin, it is currently a Proof-of-Work network, and settlement is probabilistic (yet generally considered final within a few minutes). Miners have a slightly greater ability to interfere with end-users because in some cases they can extract economic value from reordering transactions,[30] but this is not a significant hindrance to the network at present. Like Bitcoin, Ethereum transactions are generally final (with some high-profile exceptions[31]), a property that enables desirable features like composability and atomicity.[32]

Unlike Bitcoin, Ethereum is Turing-complete, which means the system can be programmed to solve any reasonable computational problem assuming sufficient memory and resources are available.[33] The trade-off for this richer and more expressive feature is costlier validation[34] and greater potential for significant bugs or loss of funds. Ethereum's programmability has made it the default destination for capital formation (i.e., the 2015-17 ICO phenomenon), third-party tokens like stablecoins, and more recently, a vibrant ecosystem of derivatives and swap products.

c. Decentralized Exchanges (or DEXs)

Ethereum, as with Bitcoin, is permissionless and does not require identity verification to make transactions. Only knowledge of a private key corresponding to an account bearing a balance on-chain[35] is necessary. As a consequence, the usage of these DEX tools, which exist primarily as publicly-visible contracts on-chain, is largely permissionless – at least at the blockchain layer

---

[30] For a discussion of how miners can extract value from reordering transactions, see Daian, Philip, et al. "Flash boys 2.0: Frontrunning, transaction reordering, and consensus instability in decentralized exchanges." *arXiv preprint arXiv:1904.05234* (2019).

[31] See Matthew Leising, "The $55m Hack that Almost Brought Ethereum Down," (Sep. 17, 2020) Coindesk. Available at https://www.coindesk.com/55m-hack-ethereum-down

[32] 'Composability' refers to the property in contracts that allow them toreference each other and enable the construction of complex interlinking systems. 'Atomicity' refers to a property of chained transactions whereby either all are completed or none are.

[33] For a more complete comparison between Bitcoin and Ethereum, see EthHub, "EthHub CFTC Response," (Feb. 15, 2019). Available at https://unlock-protocol.github.io/ethhub/other/ethhub-cftc-response/.

[34] It is more challenging for an end-user to run a node and audit the validity of an inbound transaction. Since the ability of any user to replay the history of the network is at the core of the public blockchain trust model, introducing richer computation would complicate this process of validating transactions from other parties.

[35] As compared with Bitcoin, which employs a token-based or UTXO model, Ethereum employs an account-based model.

itself.[36] While there are many other DeFi value propositions that we will cover in this essay, the notion of a DEX typifies the DeFi phenomenon. DEXes combine a reliance on third-party assets inserted on-chain, the permissionless nature of public blockchain transactions, and an insouciant attitude to financial regulations. For instance, DEXes, existing as contracts enabling users to pool liquidity and engage in bilateral trades, do not enforce KYC restrictions or identity verification.

Due to the non-custodial nature of DEX trades (as compared with deposit-taking centralized trading exchanges) and the complete lack of an obligation to share one's personal data with the network, these decentralized exchange products are extremely popular. Indeed, in August 2020, the most popular DEX, Uniswap,[37] surpassed the daily exchange volume of Coinbase,[38] the largest regulated centralized cryptoasset exchange and brokerage in the U.S. This is particularly noteworthy because Uniswap exists solely as a set of interlocking smart contracts deployed on Ethereum, depends on a decentralized network of independent liquidity providers, and boasts no infrastructure of its own aside from the Ethereum blockchain. The Uniswap contracts had been primarily written by a single individual, whereas Coinbase has hundreds of employees and has raised hundreds of millions of dollars in venture financing.

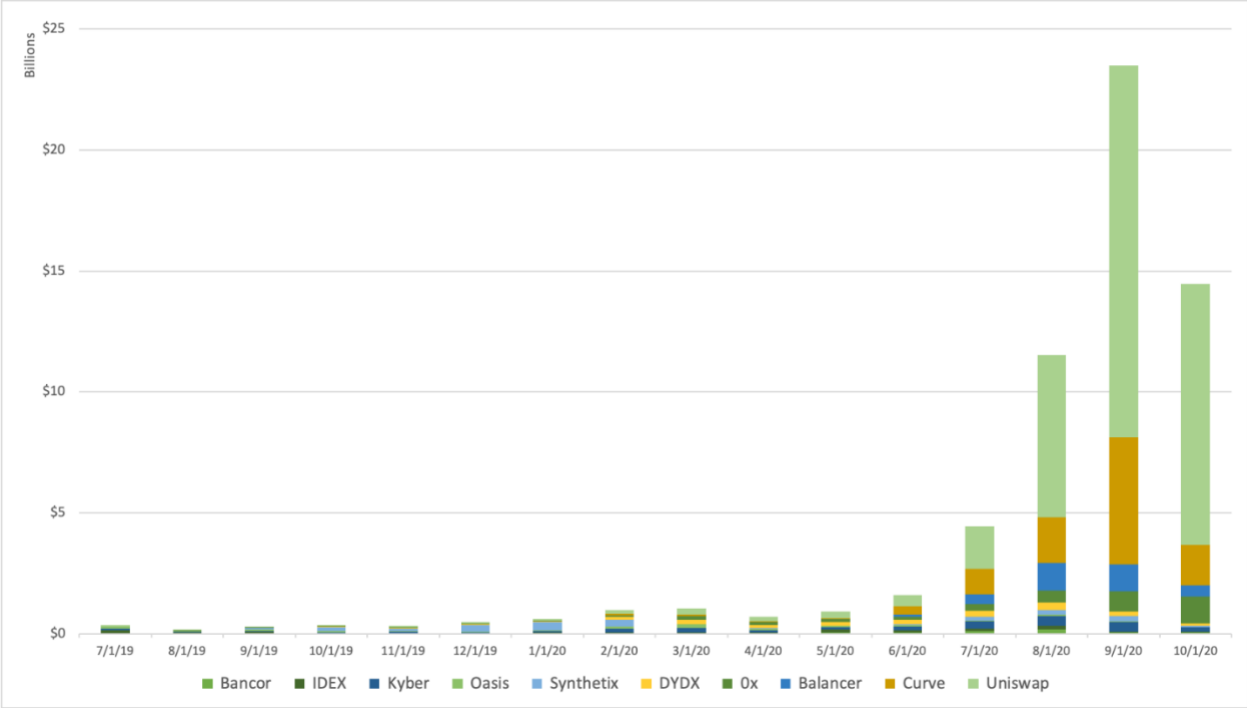
In August 2020, Ethereum-based DEXs mediated approximately $24 billion worth of transactions, each settling on-chain, with Uniswap and Curve being the most popular venues.

Figure X. Decentralized exchange volume, USD.

[36] Permissions could be inserted, for instance, at centralized on-ramps, such as exchanges, where users might seek to exchange fiat currency for cryptocurrency in order to transact within the DeFi ecosystem.

[37] For more background on Uniswap, see Olga Kharif, "DeFi Boom Makes Uniswap Most Sought-After Crypto Exchange." *Bloomberg*, (Oct. 16 2020). Available at www.bloomberg.com/news/articles/2020-10-16/defi-boom-makes-uniswap-most-sought-after-crypto-exchange

[38] Mathew Di Salvo "Trading Volume on Ethereum-Based DEX Uniswap Beats Coinbase Pro." *Decrypt*, Sept. 10 2020. Available at www.decrypt.co/40201/uniswap-24-hour-trading-volume-beats-coinbase



Source: Dune Analytics. Note: October 2020 data extrapolated from partial data.

With this background, we can summarize the extent of the decentralized finance phenomenon as it pertains to public blockchains. The core qualities offered by the DeFi sector (under the narrower conception as defined above) are as follows:

1) DeFi products are built on public blockchains like Ethereum, which grants them a robustness and resistance to shutdown that standard banking applications do not possess or aspire to. This feature, together with open source and publicly-auditable contract code, enables *trust minimization* – the notion that an end-user can theoretically audit and verify the entire system in its entirety.

2) DeFi products are *programmable*, which is to say any developer can permissionlessly deploy a set of smart contracts to the blockchain. End-users can take advantage of these deployed smart contracts by making base-layer transactions (which requires only knowledge of keys pertaining to the tokens or native cryptoassets to act as owner of the digital assets) and an interface through which to engage with the deployed smart contracts.

3) DeFi products that exist on the same blockchain are *interoperable*, which means that they work seamlessly together. Rather than having multiple databases communicate with each other (as is the case with banks and fintechs communicating via APIs), networks like Ethereum are large, unitary databases that host a large number of users[39]

[39] At the time of writing (October 2020), there were 48 million addresses on Ethereum with a nonzero Ether balance – although one address does not necessarily correspond to one individual.

and a vibrant ecosystem of financial assets. As such, communication between various financial protocols within a given blockchain is seamless. The combination of settlement qualities of public blockchain assets ”on top” of tokens circulating underneath means that these contracts can interlock cleanly with no counterparty risk that might result from unexpected settlement reversals. This feature is often referred to as “*composability*.”

4) DeFi products are, with some exceptions, *permissionless* to access – so end-users can use them without ‘know your customer’ (KYC) restrictions or other forms of identity verification. This permits more efficient applications without the burden of compliance – but remains the source of potential regulatory concern.

5) Existing as deployed contracts on public blockchains, DeFi products are transparent by design. As replicated, shared databases, transactions on blockchains like Bitcoin and Ethereum can be scrutinized by anyone with access to the data on the replicated ledger (commonly referred to as a full node). This means that individual positions can be assessed and risk in collateralized systems can be ascertained in real time. While additional privacy remains a feature that developers are seeking to add to blockchains, the transparency enables *auditability* and makes querying data on these financial products trivial.

It is worth noting that blockchain-based DeFi, which runs on single-threaded computers[40] with limited data throughput, is still crucially limited in a number of ways. Lacking a notion of on-chain identity or credit, the sector cannot replicate many of the essential features of finance or banking, like credit or underwriting.[41] Thus, while DeFi users can engage in interest rate swaps, asset pooling, and risk transformation, there is no notion of maturity transformation – converting liquid deposits into illiquid, productive capital – in the space as of yet. It is therefore critical to interpret ‘finance’ in decentralized finance in the context of what public blockchain-based systems are capable of. In this instance, it chiefly refers to the exchange of value and the transformation of risk, rather than core banking activities.

Additionally, a full conception of blockchain-based DeFi requires philosophical context. It is a movement deeply impregnated with ideology. Public blockchains are premised on a notion of disintermediation of payments and the elimination of discretion stemming from monetary systems,[42] while generally seeking to minimize state oversight and control over payments. DeFi

---

[40] Currently, the established security model that underlies Ethereum and other blockchains requires that full nodes validate the entire history of transactions. Thus, transactions cannot be parallelized; every node in the network must be aware of and process each transaction in order to have a complete, global view.

[41] For more on this see Jake Chervinsky, “DeFi Lending Doesn’t Exist Yet,” *Bankless,* Sep. 3, 2020. Available at https://bankless.substack.com/p/defi-lending-doesnt-exist-yet

[42] For insight into Satoshi’s objectives when creating Bitcoin, one ought look no further than their first post on the P2P foundation forum: “The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust.” https://satoshi.nakamotoinstitute.org/posts/p2pfoundation/threads/1/

adherents take this teleology one step further, envisioning not only novel payments systems but a rich set of financial services that a global user base can access without restriction - one in which margins are eliminated and returned to end-users as efficiencies. As Zetzsche, Arner, and Buckley describe it:[43]

> *DeFi enthusiasts go beyond technical decentralization. For them, DeFi offers governance structures they perceive as the 'democratization' of finance, while incumbents might well view such structures as 'anarchy'. At the core of this claim lies a positive connotation of disintermediation (understood as disrupting incumbent financial institutions, particularly those that are very large: the 'too-big-to-fail' problem at the heart of the 2008 financial crisis) and of decreasing state influence and control of the financial system.*

The openness facilitated by DeFi – in which a global user base, united only by their usage of public blockchain assets, can engage with complex financial contracts without restriction – is only possible absent state regulation. Thus, the core qualities listed above must be caveated in that they only pertain to the more limited functions that DeFi can plausibly claim to satisfy, and these qualities may only obtain temporarily, as regulators begin to grapple with the industry.

5. An alternative, permissionless financial system

Despite the shortcomings mentioned above, in 2020, DeFi products and ancillary business models have seen a dramatic uptick in usage, which can be directly ascertained by inspecting the blockchains themselves. The usage modes that have gained meaningful adoption thus far can be grouped into a handful of broad categories:

1) **Non-custodial exchange**: these are products that allow traders to exchange assets (typically tokens circulating on Ethereum or Ether itself) without relying on a third party for custody. Trades settle "on-chain" and are hence final. Generally, these exchanges do not require KYC, as they simply constitute software running on blockchains, allowing users to pool liquidity and define rules for exchange. Examples include Uniswap, Curve, and Balancer.

2) **Risk transformation**: this is a broad category encompassing a variety of methods to pool liquidity and transform risk. Through these products, users can borrow tokens against liquid collateral and lend out their own tokens to collect interest. Popular projects involve locking up an excess of risky crypto collateral in order to produce stable outputs, like a USD-linked stablecoin. Some of these systems use programmatic risk management and constant overcollateralization to maintain system solvency. Examples include Maker, Compound, and Aave.

[43] Zetzsche, Dirk A., Douglas W. Arner, and Ross P. Buckley. "Decentralized Finance (DeFi)." IIEL Issue Brief 2 (2020).

3) **Asset management**: these include active or passive strategies enabling users to pool funds and target a return or a specific portfolio, employing the token swapping products available on Ethereum. Examples include Melonport, Tokensets, and YFI.

4) **Programmatic derivatives**: taking advantage of the relative simplicity of expressing derivative contracts in code form, these products enable users to trade specific flavors of risk like options or bespoke derivatives, such as swaps. Examples include UMA, dy/dx, and Synthetix.

5) **Insurance**: these are products that enable users to pool risk, buy and sell insurance coverage, chiefly as protection against the failure of DeFi contracts. Examples include NexusMutual and Opyn.

6. Categories of cryptoassets in DeFi

The most popular of these protocols by usage numbers[44] are decentralized/noncustodial exchange products, as well as autonomous interest rate protocols. Additionally, while the above represent enabling infrastructure to permit a variety of financial engagements, the assets themselves circulating on these platforms have expanded – both in terms of their aggregate value and their transactional usage. The relevant assets can be demarcated as follows:

Stablecoins and DeFi

The term "stablecoins" has no official definition and generally refers to a second generation of "cryptoassets that "seek to stabilise the price of the 'coin' by linking its value to that of an asset or pool of assets."[45] Some of these stablecoins reference baskets of currencies centrally managed to maintain price stability. Certain other stablecoins - sometimes referred to as "cryptodollars"[46] - are tokens tracking the return of the US dollar (USD) and more cash-like. fFor the most part, these cryptodollars are tokenized representations of bank liabilities and are redeemable for actual USD. A smaller subset of stablecoins are issued programmatically against risky crypto-native collateral or employ other algorithmic schemes for stability. The largest fiat-convertible stablecoins include Tether, USD Coin, TrueUSD, Binance dollar, and Paxos dollar. By

[44] Usage numbers visible on-chain at Dune Analytics, available at https://explore.duneanalytics.com/dashboard/defi-users-over-time

[45] Note that 'stablecoins' can be used to refer to tokens which derive their value from their convertibility for reserves of sovereign currency held in a commercial bank, as well as non-convertible tokens whose value derives from collateral backing the asset and other stabilizing mechanisms like interest rates. For more, see G7 Working Group on Stablecoins, "Investigating the impact of global stablecoins" Bank for International Settlements (October 2019). Available at https://www.bis.org/cpmi/publ/d187.pdf

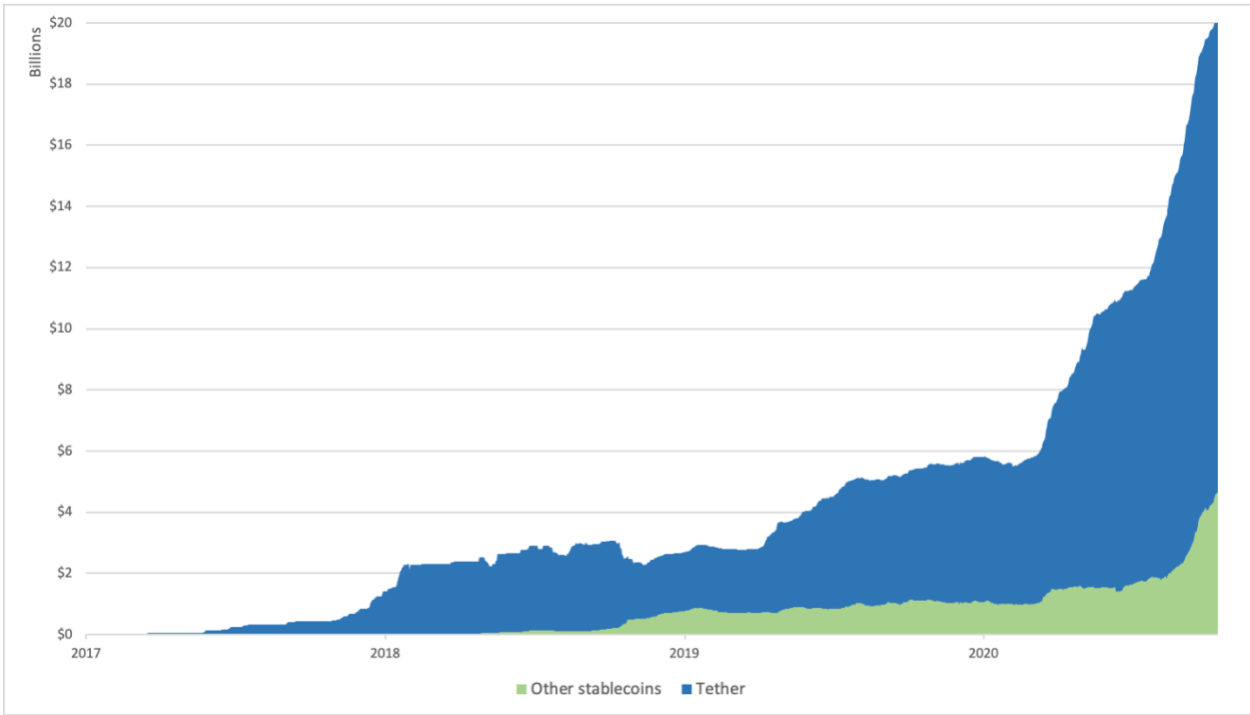
[46] For a discussion of 'cryptodollars' versus 'stablecoins', see Castle Island Ventures, "Cryptodollars: The Story so Far" (June 2020). Available at https://www.castleisland.vc/cryptodollars

contrast, the most popular synthetic stablecoins[47] issued against crypto collateral include Dai (issued against Ethereum and a basket of other tokens) and sUSD (issued against Synthetix).

The supply of stablecoins circulating on public blockchains has grown from almost zero in 2017 to over 20 billion USD today. Tether, issued against deposits in offshore banks maintains dominance, but US-based stablecoins are gaining prominence. In particular, USD Coin (USDC) issued by the Centre Consortium with reserves custodied in US banks, has grown from 520 million USD in January 2020 to 2.84 billion USD in current supply at the time of writing.

Figure X. Stablecoin free-floating market cap

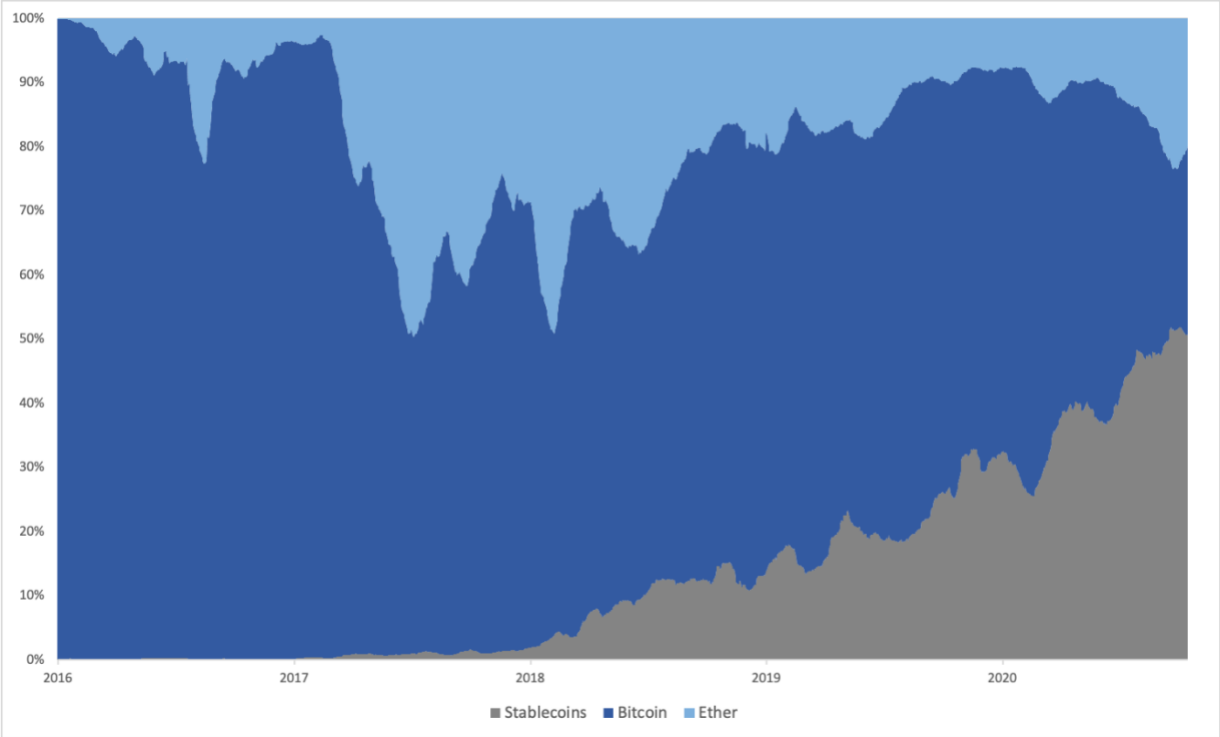
[47] For a taxonomy, see Jeremy Clark, Didem Demirag, and Seyedehmahsa Moosavi. "SoK: Demystifying Stablecoins." Available at SSRN 3466371 (2019).



Source: Coin Metrics.

Increasingly, stablecoins are displacing “native” units of these blockchains (i.e., Bitcoin and Ether) as the preferred form of collateral for these financial applications because stablecoins minimize volatility and are, thus, more suitable as media of exchange.

Figure X. Relative share of on-chain transaction value in USD terms (select cryptoassets).



Source: Coin Metrics.

Note: figure covers BTC, ETH, and select stablecoins (USDT, USDC, TUSD, GUSD, BUSD, HUSD, and DAI).

At the time of writing, stablecoins account for $4 billion USD worth of settled value per day, on a trailing 30-day basis, surpassing the combined value settled by Bitcoin and Ether. In relatively short order, these dollar-pegged tokens have become the primary transactional medium for crypto-financial applications. Fundamentally, certain stablecoins offer privacy and settlement assurances which approximate (but do not match) those of physical cash, in a digital context. They are "bearer"-like" in the blockchain sense (i.e., knowledge of the keys is tantamount to ownership) and offer individuals worldwide access to dollar IOUs representing US dollars held in commercial banks. For individuals with no access to dollar-denominated savings products, stablecoins offer the prospect of diversification from their local currency.[48] Furthermore, using interest rate swap products, users can get access to interest rates indexed to the demand for crypto-native capital, which frequently drives rates well above the risk free rate.[49] Effectively, stablecoins, in conjunction with a liquid and accessible money market on DeFi, grant users access to dollar-denominated finance, regardless of the nature of their local banking sector.

[48] Although, it's worth noting that the legal entitlements of the owners of stablecoins differ by issuer and generally do not include FDIC deposit insurance unlike domestic commercial bank deposits.

[49] Real-time cryptocurrency interest rates for both centralized and decentralized lending facilities visible at Defirate: https://defirate.com/lend/

Unlike the "native" units of currency on these blockchains, fiat-convertible stablecoins are more accountable to the traditional banking system and to regulators. The issuers behind stablecoins like Tether and USDC reserve the right to blacklist addresses should they get a request from law enforcement or in the case of a hack, and they actively take advantage of this functionality.[50]

To create or redeem a fiat-convertible stablecoin, an entity must have a direct relationship with the issuer and pass sufficient KYC. However, most stablecoin transactions are P2P directly on the blockchain , taking place between end-users who have no obligation to furnish any identity information, so stablecoin issuers have limited sight into P2P transactions on-chain. This particular model, whereby creations and redemptions occur with known counterparties, but the majority of transactions are opaque to stablecoin administrators, has been dubbed "permissioned pseudonymity."[51]

Whether this permissioned pseudonymous risk model – which departs significantly from that employed by payments companies, like PayPal, that are aware of every transaction on their networks – can persist in perpetuity is an open question. The Financial Action Task Force (FATF) noted pointedly in their recent *12 Month Review* that "the lack of explicit coverage of peer-to peer transactions via private / unhosted wallets was a source of concern for a number of jurisdictions,"[52] adding, seemingly in reference to more decentralized stablecoins like Dai, "there are residual risks relating to anonymous peer-to-peer transactions via unhosted wallets, jurisdictions with weak or non-existent AML/CFT regulation and so-called stablecoins with decentralised governance."[53] If stablecoin administrators must progress from the very occasional blacklist model to a more aggressive blacklist policy, or even a whitelist approach where they are required to collect identity data on every token transfer, stablecoins will lose a core element of their value proposition – less encumbered digital cash-like transactions on public infrastructure.

Liability-free cryptoassets

"Native" cryptoassets constitute the base of DeFi. Initially employed as the sole media of exchange, these cryptoassets have become widely employed as collateral. Ether is the default asset on Ethereum, but over $1 billion USD of wrapped Bitcoin also circulates within DeFi

---

[50] The blacklisted addresses on Tether can be tracked in real-time at Dune Analytics, available at https://explore.duneanalytics.com/public/dashboards/3zhIaRUCFgmZMKqHG0pguvSvw1aOGL8gxFtZ2ujf. USDC has also begun freezing addresses at the behest of law enforcement.

[51] For more on permissioned pseudonymity, see JP Koning "From Unknown Wallet to Unknown Wallet," *Moneyness blog*, Nov. 6 2019. Available at https://jpkoning.blogspot.com/2019/11/from-unknown-wallet-to-unknown-wallet.html and Antony Lewis, "KYC in Stablecoins," *Bits on Blocks*, available at https://bitsonblocks.net/2019/10/30/kyc-in-stablecoins/.

[52] Financial Action Task Force, "12 Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers," June 2020. Available at https://www.fatf-gafi.org/media/fatf/documents/recommendations/12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASPS.pdf

[53] Ibid, p 17

applications on Ethereum. Currently, 8.6 million Ether and 158,000 BTC are held as collateral in DeFi applications, equivalent to $3.2 billion USD and $1.7 billion USD, respectively at the time of writing.[54] When employed as collateral in DeFi systems, users in some cases surrender immediate control of their coins – for instance, if they use their coins to provide liquidity to an automated market maker exchange in exchange for a return – but they retain ownership and can withdraw their coins at their discretion. Given that native cryptocurrencies like Bitcoin and Ether are not guaranteed or backstopped by any third party, but instead have a solely market-determined value, they make suitable collateral for these systems. Since these protocols are credibly decentralized, users can transact freely and engage with decentralized finance products in a relatively unconstrained manner without fear of censorship.

Pseudo-equity

Lastly, a final class of tokens circulating within the DeFi ecosystem can be understood as ersatz or primitive equity products. These are assets which derive their value from control rights and underlying cash flows accruing to DeFi protocols. For the most part, these are not issued under established securities law processes, do not involve traditional disclosure norms that public markets investors might expect, and are not formally attached to a corporate entity. However, many of these tokens confer some of the rights associated with conventional equity securities, giving rise to the pseudo-equity appellation.

Issuance and liquidity for pseudo-equity is facilitated by the presence of decentralized exchange products, providing a global audience of investors access to these products without reliance on centralized, regulated exchanges. The issuance and exchange of pseudo-equity motivate end-users to engage with DeFi products (in particular, DEX products), which in turn contributes to their popularity (because pseudo-equity can be contractually associated with DeFi projects and, thus, derive fees and cash flow from the contractual arrangements).

6. Systemic risk: is genuine openness a poisoned chalice?

The features that render DeFi more fundamentally 'open' than traditional financial networks involve considerable tradeoffs. There are a number of issues present in DeFi that established financial institutions face to a lesser degree; chiefly, these involve pitfalls involved in transacting with digital bearer assets, the possibility of systemic failures due to interconnectedness, and the constant specter of enforcement due to a general rejection of identity-based compliance processes.

Incorporating digital bearer assets can be extremely costly to users who lose keys. By design, there is no recourse for key loss. The flipside of composability is potential cascading failures if a key lynchpin fails. Convertible fiat-backed tokens are a clear potential point of compromise

[54] Data courtesy of DefiPulse. Available at defipulse.com

here, since they account for a significant fraction of the collateral backing DeFi products. At the time of writing, $422 million USD worth of USDC is being employed as collateral in Maker,[55] against which Dai is issued. However, as Dai is largely unregulated and Maker is more decentralized in nature, no freezing function exists, as is the case with USDC and Tether. Thus, if Centre were ever pressured to eliminate the USDC from the asset pool backing Dai and to freeze the USDC collateral, the system could become insolvent or otherwise impaired. Since Dai is considered to be a credible, censor-resistant, low-volatility asset, it is widely employed in other DeFi protocols. Thus, a compromise of its underlying collateral (which could spark a rapid devaluation) would have knock-on effects on other DeFi protocols. The nature of such extreme interconnectedness is such that the failure of a single popular component can be systemic.

Another issue with the permissionless and unrestricted pooling of assets that is common within DeFi is the potential for systemic 'taint' if coins associated with illicit activity enter a pool. This raises difficult questions for participants in the pool, counterparties in transactions, and the developers maintaining the pooling software. This question has yet to be seriously explored within the DeFi sector.

Additionally, open questions linger around the legal treatment of stablecoins and the quality of their settlement assurances, and the rights of token holders in a situation of liquidation, collateral impairment, or distress. Unlike deposits at commercial banks, stablecoin balances are not federally-insured. Since stablecoins have become the most widely-used medium of settlement within DeFi, the sector is now more vulnerable to pressure, especially through the centralized administrators and banks holding the reserves backing the DeFi system.

Financial crimes enforcement agencies have taken notice of the DeFi phenomenon and have made it clear that they plan to grapple with it. The U.S. Department of Justice, in their recent *Cryptocurrency Enforcement Framework*, mentioned the sector specifically as a topic of interest, noting that "decentralized platforms, peer-to-peer exchangers, and anonymity-enhanced cryptocurrencies that use non-public or private blockchains all can further obscure financial transactions from legitimate scrutiny."[56] Indeed, precedent stemming from the EtherDelta settlement[57] with the U.S. Securities and Exchange Commission (SEC) suggests that securities regulators consider decentralized exchange administration to be a covered activity, in particular if these contracts are facilitating the exchange of unregulated securities.

While public blockchains do not require user identities to operate, opting instead for a pseudonymous model, they also explicitly reject KYC as part of an ideological commitment to privacy and digital cash. Nonetheless, identity is gradually being reinserted into these systems.

---

[55] Data found at Dune Analytics. "Maker DAO MCD," Dashboard by Fredrik Haga, available at https://explore.duneanalytics.com/dashboard/maker-dao---mcd

[56] "Cryptocurrency Enforcement Framework," Report of the Attorney General's Cyber Digital Task Force, U.S. Department of Justice, Oct. 2020. Available online at https://www.justice.gov/ag/page/file/1326061/download

[57] "SEC Charges EtherDelta Founder With Operating an Unregistered Exchange," Securities and Exchange Commission, Aug. 25 2018. Available at https://www.sec.gov/news/press-release/2018-258

Centralized exchanges are the primary points where users initially acquire the cryptoassets, and these centralized exchanges represent the best opportunity for regulators to tie blockchain addresses to individuals. The FATF's Travel Rule[58] stipulates that user data must travel with withdrawals from Virtual Asset Service Providers (VASPs), and is gradually coming into effect on a jurisdiction-by-jurisdiction basis. The question for the industry is whether these novel requirements require disclosing one's own blockchain address when withdrawing from a VASP, as is the case in Switzerland.[59] As public blockchains remain largely traceable, disclosing one's on-chain identity is tantamount to surrendering financial privacy. If this model were to become the default, and VASPs (and the governments regulating them) were able to characterize most on-chain addresses and tie them to user identities, the permissionless nature of DeFi would be significantly eroded, and so would its core value proposition.

Chainalysis estimates[60] that 60 percent of bitcoins that are not lost are held by licensed exchanges. With offshore and largely unregulated exchanges like BitMEX being targeted by the Department of Justice and the Commodity Futures Trading Commission (CFTC),[61] the fraction of exchanges – and hence users of cryptocurrency – that is accountable to engaged regulators is growing.

If financial regulators are able to tie individuals to blockchain transactions, they will eventually seek to regulate DeFi processes to the extent that they touch their mandates. Given that DeFi protocols reject KYC and other forms of authentication and require only ownership of digital assets, more regulatory attention appears inevitable. Thus, the longevity of the current regime of radical openness and low compliance barriers in the blockchain-based DeFi space remains questionable.

7. Prospects for the convergence of decentralized and traditional finance

As the scope and intensity of blockchain-based transactional activity grew, its collision with the traditional financial sector was inevitable. Early on in Bitcoin's history, U.S. banks refused to do business with digital currency exchanges, but as attitudes moderated and the core technology

---

[58] See Recommendation 16. Financial Action Task Force, "Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers" (June 2019). Available at https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html

[59] Ciphertrace CEO Dan Jevans explains the Swiss interpretation of the Travel Rule on the Unchained podcast, stating "[the Swiss government] is extending it to self-custodial wallets where you have to make declarations about who you are. So they've taken it beyond VASP to VASP. They're stretching the boundary [and] extending it to more self-custodial wallets." See "Why The Travel Rule Is One Of The Most Significant Regulations In Crypto" *Unchained Podcast*, Aug. 4 2020. Available at https://unchainedpodcast.com/why-the-travel-rule-is-one-of-the-most-significant-regulations-in-crypto/

[60] "60% Of Bitcoin Is Held Long Term as Digital Gold. What About the Rest?" *Chainalysis Blog*, June 18, 2020. Available at www.blog.chainalysis.com/reports/bitcoin-market-data-exchanges-trading

[61] "CFTC Charges BitMEX Owners with Illegally Operating a Cryptocurrency Derivatives Trading Platform and Anti-Money Laundering Violations," CFTC, Oct. 1, 2020. Available at https://www.cftc.gov/PressRoom/PressReleases/8270-20

became better understood, Tier I banks began to service these entities.[62] The prospects for integration brightened in the U.S. with two letters from the Office of the Comptroller of the Currency, one clarifying that federally-chartered banks could provide custody services for cryptoassets,[63] the other ratifying a status quo whereby banks were holding dollar reserves for stablecoin issuers.[64] This guidance provides strong clarity for banks to begin to incorporate public blockchains as an additional settlement network.

Additionally, crypto exchanges have begun to pursue bank charters under Wyoming legislation creating Special Purpose Depository Institutions (SPDI).[65] Kraken Financial, a subsidiary of Kraken, a long-running cryptoasset exchange, was the first entity to receive the SPDI charter and may apply for access to the federal payment system at the local regional branch of the Federal Reserve System.[66] Either through crypto-native institutions leveraging the Wyoming legislation for access to base money or via established banks building crypto custody products, the emergence of a novel class of financial institutions which engage with cryptocurrency while maintaining direct access to the Federal Reserve System is a genuine prospect.

One novel dimension of blockchain-based assets is their portability. Users can take self-custody of their assets without relying on a third party. In this paradigm, exchanges and brokers are relegated to mere interfaces, as opposed to the sole and fundamental means of engagement with one's assets. The ease of withdrawing one's funds – compare this with withdrawing gold from a vault or securities from a broker – means that service providers covering cryptoassets face the continual prospect of asset flight, which acts as a disciplinary force. After a series of aggressive liquidations on the Bitcoin derivatives exchange BitMEX in March 2020, traders withdrew 103,000 BTC from the exchange in under a month, worth over $1 billion. These dramatic asset flows are facilitated by the ease of undertaking physical settlement, and portend a competitive and mercurial environment for custodians and brokers.

Additionally, as ambitions to create central bank digital currency (CBDC) expand, the installed base of fiat-convertible tokens circulating on-chain could be leveraged for a hybrid model. While the eventual nature of a US CBDC is still in question, domestic stablecoin issuers could

---

[62] In 2020, JP Morgan announced that they would provide banking services to crypto exchanges and custodians Coinbase and Gemini. See Paul Vigna. "JPMorgan Extends Banking Services to Bitcoin Exchanges." *The Wall Street Journal*, Dow Jones & Company, May 12 2020, www.wsj.com/articles/jpmorgan-extends-banking-services-to-bitcoin-exchanges-11589281201

[63] "Federally Chartered Banks and Thrifts May Provide Custody Services For Crypto Assets." Office of the Comptroller of the Currency, July 22 2020, www.occ.gov/news-issuances/news-releases/2020/nr-occ-2020-98.html

[64] "Federally Chartered Banks and Thrifts May Engage in Certain Stablecoin Activities." Office of the Comptroller of the Currency, Sept. 21 2020, www.occ.gov/news-issuances/news-releases/2020/nr-occ-2020-125.html

[65] For more detail on the Wyoming SPDI, see "Special Purpose Depository Institutions," *Wyoming Division of Banking*, available at http://wyomingbankingdivision.wyo.gov/home/areas-of-regulation/laws-and-regulation/special-purpose-depository-institution

[66] For more on Kraken's SPDI approval, see: "The First Cryptocurrency Bank." *The National Law Review*, Sept. 22, 2020, available at www.natlawreview.com/article/first-cryptocurrency-bank

advocate for a public-private partnership in which they continue to maintain relationships with their userbase and facilitate peer-to-peer, cash-like transactions, while backing the fiat IOUs circulating on-chain with high-quality base money. This would be an improvement from a reserve quality perspective from the current model based on commercial bank liabilities.

Already, major fintechs have embraced public blockchain assets,[67] albeit with varying levels of functionality. While Square's Cash App permits Bitcoin deposits and withdrawals, Robinhood, PayPal, and Revolut offer financial exposure but not direct access to the underlying assets. Increasingly, fintechs are taking notice of the presence of blockchain-based assets in the portfolios of their users, and have begun to incorporate blockchain accounts – both directly on-chain, and at custodial exchanges – into financial tracking. Account aggregation is trivial for on-chain addresses, as the entire history of activity is present on the public ledger; sharing a blockchain address is typically sufficient to draw in a user's transactional history. Fintechs or neobanks offering high yield savings products may also be enticed by the structurally-high yields available in the cryptodollar lending space. Already, uninsured money market accounts offering users access to DeFi yields in a familiar interface have emerged.

Lastly, securities offer a final point of incipient integration between decentralized and traditional finance. Developments like Ethereum's ERC-1404 standard[68] permit the whitelisted trading of assets, allowing users to transfer security claims on a public blockchain without risking their distribution to unauthorized parties. Already, the SEC has permitted the issuance of securities on Ethereum through this standard,[69] indicating their openness to the presence of securities on public blockchains, provided the existence of certain constraints. These tokens could plausibly be employed in existing DeFi infrastructure, mirroring the existing securities-backed lending industry, this time in an on-chain and automated context.

Fundamentally, public blockchains and the emerging suite of financial products built atop them aspire to be decentralized and disconnected from the established financial system. However, user demands for intermediated services like custody, alongside the growing importance of the industry, have caused a natural convergence with the financial sector to take place. As mentioned however, the permissionless and unencumbered nature of blockchain-based DeFi can make for an uneasy marriage with regulated institutions. Nonetheless, blockchain-based DeFi can serve as the foundation for rich ecosystems of ever-evolving services and products.

Conclusion

---

[67] Major fintechs offering crypto products include Robinhood, PayPal, eToro, Square's Cash App, Mogo, Hype, SoFi, and TradeStation.

[68] For more on ERC-1404, see Tokensoft's Erc1404.org, available at: https://erc1404.org/

[69] The securities in question are ArCoin (For more on ArCoin, see Danny Nelson. "605 Days Later: How ArCoins Got the SEC Go-Ahead as an Ethereum-Traded Treasurys Fund." *CoinDesk*, 29 July 2020, www.coindesk.com/arcoins-blockchain-traded-fund-arca-tokensoft and INX (See SEC Form F-1, "Registration Statement", INX Limited. Aug 19, 2020. Available online at https://www.sec.gov/Archives/edgar/data/1725882/000121390019016285/ff12019_inxlimited.htm)

As we have shown, public blockchain-based DeFi is motivated by many of the same ideals that underscore the open finance movement: interoperability, granting better outcomes for users of financial services by stimulating competition service providers, and providing the ability to freely move between providers. These objectives are implemented in different ways. Open finance is concerned with linking established financial firms and fintechs and creating protocols to share user-permissioned data; decentralized finance envisions an entirely novel and distinct financial system built atop public blockchains, in which users primarily self-custody their assets and interact with autonomous, clearly-specified open source financial applications.

At its current stage, public blockchains like Ethereum conjoin tens of millions of users worldwide on a single replicated database. This enables seamless composability between different financial applications which reference each other freely. Open finance and open data by contrast must reckon with installed financial plumbing and involves finding communication bridges between bank databases. DeFi may face a paradox if liquidity becomes more fragmented across blockchains, or Ethereum scales by distributing transactions to multiple subledgers which periodically reconcile – it risks losing the composability advantages which are its selling point, especially with regards to more complex financial applications.

In my view, the products offered by decentralized finance have reached a level of maturity where they are challenging established financial infrastructure. Much of the enthusiasm for DeFi is predicated on its repudiation of identity-based compliance, as well as the strong portability of assets between distinct financial products, and the ability of end-users to retain custody of their assets. The promise of permissionless innovation in financial services for a global audience, without requiring bank charters or onerous regulatory oversight, has driven a wave of activity in the sector. Whether the open qualities of DeFi can endure is the sector's existential question. Its genuine permissionless quality – its key value proposition – may have to be dialed back, as regulators turn their gaze to DeFi, and it becomes further integrated with the established financial system.